THE INTERNET OF THINGS (IOT): CONSUMER APPLICATIONS

Medvedev S. V.
Belarusian State University of Informatics and Radio electronics
Minsk, the Republic of Belarus

Andreeva O. V

This article is devoted to the Internet of Things and describes it in the broadest sense. The detailed analysis of the Internet of Things consumer support is given. To finish with negative aspects of the Internet of Things are shown.

In the most common sense, the term IoT describes everything connected to the one network. Professionally speaking, the Internet of things (IoT) is a network of interrelated computing devices, mechanical or digital machines provided with exclusive marking and abilities to transfer data over connections without human interference. The billions of media around the globe that are connected throughout the Internet Web serve as a brilliant example of this technology. The earliest technology development dates as far back as the end of 20th century. The idea of complementing basic objects with sensors and intelligence was discussed during the 80s and 90s, however, the advancement of these early projects was slow, just because the technology at the time wasn't ready [1]. Chips were too bulky and objects could not communicate so effectively.

The IoT promises to change our environment — our homes, workplaces and vehicles will be smarter and even chattier. Smart speakers such as Amazon's Echo and Google Home already make it easier to listen to music, set alarms or find information. Home security systems help monitor what is happening on the inside and the outside of our homes, see and talk to visitors. Meanwhile, a smart lightbulb makes it look like we are home even when we are out.

Manifestation of these ideas appears to be the concept of a smart home. For buyers, this particular technology is, probably, where they are likely to get to know internet-enabled devices, and it's market which all the major companies (in particular Amazon, Google, and Apple) are vying hard for. IoT devices perfectly play into the concept of the home automation, which includes lighting, heating and air conditioning, media and security systems. Long-term effects could be seen as energy savings by automatic lights and electronics turning off on their own.

Smart homes are also provided with additional safety improvements. The features can include sensors monitoring for medical conditions and emergencies such as falls or heart attacks. Smart home devices adopted in this way provides elderly users with a higher quality of life.

Furthermore, there are many applications for the Internet of Things. Medical usage of the IoT includes healthcare related utilities, data flow and analysis are essential for monitoring and controlling situations for each of patients medical conditions. The "Smart Healthcare", as the Internet of Medical Things has been referred to, has an ability of creating a digitized system, connecting available resources and medical services [2]. Hospitals already have started utilizing "smart beds" that detect whether they are occupied or not and when patients are leaving their positions. It also adjusts itself to provide the pressure and support needed to be applied to the patient without medical staff. A 2015 Goldman Sachs report showed that IoT devices "can save the United States more than $300 billion in annual healthcare expenses by increasing income and decreasing cost".

With all the sensors, the IoT is surely to become a big privacy and security threat. While firms make fortune from selling you the smart object initially, their business models probably involve selling some of the data, too. What happens to that information is a serious debate matter. Not all smart companies dedicate their business model to selling your data, but some do [3].

Governments and consumers are growing increasingly concerned about the risks here. The UK government has released its own guidelines and requirements for the security of distributed IoT devices. It expects electronics to have their own unique passwords, be resistant to hackers' attempts to steal your personal data; also, companies are to provide a public point of contact so users will be able to report a found flaw, and that manufacturers announce when their devices get new security updates. It is quite a modest list, but undoubtedly a necessary start.

References:

1. Zdnet [Electronic resource] – Mode of access: https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ – Date of access: 20.02.2020.

2. Encyclopedia Britannica: in 15 vol. / ed: Theodore Pappas. – Encyclopedia Britannica Inc., 2010– vol. 12. – P. 324-327

3. Wired.com [Electronic resource] – Mode of access: https://www.wired.com/story/wired-guide-internet-of-things/ – Date of access: 20.02.2020.